ADVANCES IN APPLIED MATHEMATICS 7, 344–380 (1986)

Multiplicative Characters and the Discrete Fourier Transform*

R. TOLIMIERI

Department of Electrical Engineering, City College, New York, New York 10031

Multiplicative character theory will be used to reprove results from a paper of Auslander–Feig–Winograd (*Adv. in Appl. Math.* **5** (1984), 31–55) on the multiplicative complexity of the discrete Fourier transform. The Fourier transform F_A acting on the space $L(A)$ of all complex-valued functions on $A = Z/n$, n an integer, is decomposed relative to "rational" subspaces of $L(A)$ naturally described by multiplicative characters of A. This decomposition is the main tool needed to understand the ad hoc constructions in the Auslander–Feig–Winograd (op cit.) paper.

INTRODUCTION

The construction of algorithms computing

$$y = F(n)(x), \qquad x \in \mathbb{C}^n, \tag{1}$$

where $F(n)$ is the $n \times n$ Fourier transform matrix

$$F(n) \equiv [w^{jk}]_{0 \le j,k < n}, \qquad w = \exp(2\pi i/n), \tag{2}$$

is of great importance in digital signal processing. As practical demands require larger and larger size computations, often in real time, the need for increased computational efficiency has resulted in new technology both in hardware and in software. The matching of these parallel developments can be the most difficult part of the problem. Even within a given hardware technology, there can be many ways of arranging computations. On the other hand, a theoretic algorithm must eventually be judged on its ability to be implemented in practical situations. The judgement can, eventually, be made relative to existing hardware but also by its ability to point the way to new hardware development.

*Research supported in part by the NSF.

0196-8858/86 $7.50

In this work, we will study a recent work of Auslander, Feig, and Winograd [1] from a number theoretic point of view. Although, there is a price to be paid in developing some background material, once done, the algorithms of [1] can be constructed in a straightforward fashion. We believe that our approach yields new insight in our understanding of these algorithms and of multiplicative algorithms in general. In any case, knowing an algorithm from several points of view can be essential for its eventual implementation.

The role of the multiplicative structure of $\mathbb{Z}/n$ as a tool for computing (1) can be found in Rader [2] when $n = p$, p a prime, and in Winograd [4] when $n = p^m$, p a prime, and $m \geq 1$. We will need the following definition. A computation of the form

$$v = Q_1 F(n) Q_2 u, \qquad u \in \mathbb{C}^n, \tag{3}$$

where Q_1, Q_2 are rational, nonsingular matrices, is called rationally similar to computation (1). Any algorithm computing (3) can be modified, using only rational operations, to compute (1). Winograd's methods, begun in [4] and culminating in [1], use the multiplicative structure of $\mathbb{Z}/n$ and matrix multiplications to show the existence of rational, non-singular matrices Q_1 and Q_2 such that $Q_1 F(n) Q_2$ has a block diagonal form, where each block can be identified with multiplication in some quotient polynomial algebra. For details, see [1, pp. 100–101]. Highly efficient algorithms can be used to carry out these computations. The final form of these techniques, since it involves cyclotomic fields, suggests the crucial role played by number theoretic concepts. Part of the goal of this work is to make explicit how number theory enters. In Section 1, the ring $\mathbb{Z}/n$, $n = p^m$, $m > 1$, and p an odd prime is studied. The case $p = 2$ can be handled in a slightly modified way. See [3, 1], for details. Since p is an odd prime, the group of units U of $\mathbb{Z}/n$ is a cyclic group. The set $\mathbb{Z}/n$ should be viewed as the indexing set of n-point data. A fundamental partitioning of $\mathbb{Z}/n$ into U-orbits is given. The "multiplicative" partitioning of data along with the cyclic group property of U plays a crucial role in Winograd's theory which we review in Section 2. A complete developement of Winograd's result appears in [4].

The ideal theory of $\mathbb{Z}/n$ is considered next. The critical result is that $\mathbb{Z}/n$, for $n = p^m$, $m > 1$, is a local ring. Thus, $\mathbb{Z}/n$ has a unique maximal ideal, denoted by M and given by $M \equiv p\mathbb{Z}/n$, which is the set complement of U of $\mathbb{Z}/n$. As a consequence, the U-orbits if $\mathbb{Z}/n$ can be described by set difference of powers of M.

In Section 3, we begin examining the structure of the Fourier transform, especially the deep relationship between the Fourier transform and the ideals of $\mathbb{Z}/n$. Unifying concept is taken to be a bilinear pairing of $\mathbb{Z}/n$. The bilinear pairing leads to a duality of $\mathbb{Z}/n$ which pairs together ideals.

This simple but fundamental result has an important function theoretic consequence which we will now describe. Let $L(\mathbf{Z}/n)$ denote the complex vector space of complex valued functions on $\mathbf{Z}/n$. Thus, $L(\mathbf{Z}/n)$ is the space of n-point data or more precisely, periodic data modulo n. The Fourier transform F of $\mathbf{Z}/n$ is defined as a linear isomorphism of $L(\mathbf{Z}/n)$. Although our definition of F is standard, we have emphasized its dependence on the bilinear pairing. The function theoretic analog of the duality between ideals is given in Theorems 1 and 2. The usual notion of periodic and decimated functions in $L(\mathbf{Z}/N)$ are given relative to the ideals. Then, in part, Theorems 1 and 2 assert that the Fourier transform of a periodic function, periodic relative to some ideal, is a decimated function relative to the dual ideal. The converse is also true.

These results naturally lead to the definition of certain subspaces of $L(\mathbf{Z}/n)$ by periodicity and decimation conditions. We single out one of these subspaces, denoted by $L(1, m-1)$ in this section. It turns out that $L(1, m-1)$ is invariant under F and that the restriction of F to $L(1, m-1)$ can be identified with the Fourier transform of $\mathbf{Z}/p^{m-2}$. Used as an induction step, the result reduces the study of F to the study of F on the orthogonal complement of $L(1, m-1)$.

In Section 4, we introduce the main innovation of this work, the multiplicative characters of $\mathbf{Z}/n$. In [3], multiplicative character theory was used to construct an orthonormal basis diagonalizing the Fourier transform. Let $\hat{U}$ denote the set of multiplicative characters. Essentially, $\hat{U}$ is the function theoretic analog of U. In fact, $\hat{U}$ has a natural group structure isomorphic to U. The set $\hat{U}$, which we view as a subset of $L(A)$, will be partitioned by periodicity conditions. The important subset of primitive multiplicative characters is defined.

In Section 5, we study the action of the Fourier transform F on multiplicative characters. The first results are global, depending on the duality between periodicity and decimation determined by F and certain orthogonality conditions satisfied by multiplicative characters and their Fourier transforms. Subspaces defined by periodicity and decimation conditions are related to subspaces spanned by subsets of multiplicative characters and the Fourier transform of such subsets. The above-mentioned partitioning of $\hat{U}$ plays a major role. In particular, we construct an orthonormal complement C of $L(1, m-1)$ from the orthogonal set $\hat{U} \cup F(\hat{U})$. To complete this stage of our analysis of F we derive explicit formulas describing the action of F on multiplicative characters.

The theory built in the preceding section will be applied to understanding the results in [1]. The important concept of a rational subspace of $L(\mathbf{Z}/n)$ is defined and and we show that the subspaces built from sets of multiplicative characters and sets of their Fourier transforms are rational subspaces. Using this major result, we rationally modify F such that, denoting the

rationally modified F by F', we have that each of these rational subspaces os F'-invariant. Finally, we use the Chinese remainder theorem to show that F' restricted to each of these rational subspaces is polynomial multiplication in a quotient polynomial algebra. This completes the picture and gives the theoretical machinery underlying the algorithms of [1].

1. The Ring $\mathbb{Z}/n$

Take a prime integer $p \neq 2$. Form the ring

$$A(m) \equiv \mathbb{Z}/p^m, \qquad m \geq 1 \tag{1}$$

of integers mod p^m. In this section we will describe, usually without proof, several important properties of the ring $A(m)$. The multiplicative group $U(m)$ of units of $A(m)$ plays a central role. We will make the identification

$$A(m) = \{ j \in \mathbb{Z} : 0 \leq j < p^m \}. \tag{2}$$

Under this identification, we have

$$U(m) = \{ j \in \mathbb{Z} : 0 \leq j < p^m, p \nmid j \}. \tag{3}$$

The ring $A(1)$ is a field and the group $U(1)$ is a cyclic group. The Rader–Winograd algorithm computing

$$F(p)v, \qquad v \in \mathbb{C}^p, \tag{4}$$

depends, in part, on the property of the group $U(1)$.

For $m > 1$, the ring $A(m)$ is not a field, but since we are assuming that p is an odd prime, we still have that $U(m)$ is a cyclic group. This fact plays an important role in Winograd's algorithm for computing

$$F(p^m)(v), \qquad v \in \mathbb{C}^n, \ n = p^m. \tag{5}$$

In this section we will define $U(m)$-orbits of $A(m)$ and construct a partition of $A(m)$ into $U(m)$-orbits. This partition is fundamental to Winograd's work and will play an equally important part in our theory. The ideal theory of $A(m)$ will be studied. We will show that $A(m)$ is a local ring. As a consequence, the $U(m)$-orbits and the ideals of $A(m)$ are closely related. This is an essential result for our theory, since as we will subsequently see, the Fourier transform is tied to ideal theory and our main tool for studying the Fourier transform, which is the multiplicative characters of A introduced in Section 4, is most naturally associated to the group $U(m)$.

For $1 \leq r < m$, we can consider the ring $A(r) \equiv \mathbb{Z}/p^r$ and associate $A(r)$ to $A(m)$ in two ways. First we define a group isomorphism σ_r of $A(r)$ into $A(m)$, called a decimation. In Section 3, we will relate the decimation

σ_r to the standard decimation of data concept. We also define a ring homomorphism π_r of $A(m)$ onto $A(r)$, called a periodization. The role of the periodization π_r to periodic data can be found in Section 3 as well.

Set $A \equiv A(m)$ and $U \equiv U(m)$ in the following discussion. Under addition, A is an abelian group and inherits the structure of a $\mathbf{Z}$-module. If $a = j + p^m\mathbf{Z}$, $j \in \mathbf{Z}$, is any element of A, then

$$ka = kj + p^m\mathbf{Z}, \qquad k \in \mathbf{Z}. \tag{6}$$

For $0 \leq k \leq m$, define the subsets D_k of A by setting

$$D_k \equiv p^k U \tag{7}$$

and call D_k the U-orbit of p^k. By the identification (3), we can describe D_k as

$$D_k = \{0 \leq j < p^m,\ p^k | j,\ p^{k+1} \nmid j\}. \tag{8}$$

Each element $a \in D_k$ can be uniquely written as

$$a = p^k s, \tag{9}$$

where $0 \leq s < p^{m-k}$ and $(p, s) = 1$.

The U-orbits determine a partition of A, in the sense of

1. $D_k \cap D_r = \varnothing$, for $r \neq k$;
2. $A = \bigcup_{k=0}^{m} D_k$.

This partition of A, referred to at the beginning of the section will be used in Section 2 to give a partitioning of data, indexed by A, consistent with the ring structure of A.

We will now study the ideal theory of the ring A. The U-orbits can be described in terms of the ideals of A.

The field $A(1)$ contains no non-trivial ideals. We will assume in the following discussion that $m > 1$. Define

$$M(m) \equiv pA. \tag{10}$$

Set $M \equiv M(m)$. Using the identification (2), we can write

$$M = \{pk: 0 \leq k < p^{m-1}\}. \tag{11}$$

Direct verification shows that M is an ideal of A. By (5) and (11), we have

$$A = M \cup U, \tag{12}$$

$$M \cap U = \varnothing. \tag{13}$$

Every ideal of a ring is disjoint from the unit group of the ring. It follows from (12) and (13) that M contains every ideal of A and M is the unique

maximal ideal of A. A ring having a unique maximal ideal is called a local ring. For $0 \leq j < m$, define the ideal M^j of A by setting

$$M^j \equiv p^j A \tag{14}$$

By (2), we can write

$$M^j = \{ p^j k : 0 \leq k < p^{m-j} \}. \tag{15}$$

Every ideal of A is of the form M^j, $0 \leq j \leq m$. The ideal structure of A is especially simple. In fact, we have

$$(0) \subset M^{m-1} \subset \cdots \subset M^2 \subset M \subset A. \tag{16}$$

Form the set differences, $M^j - M^{j+1}$, $0 \leq j < m$; by (8) and (11),

$$D_j = M^j - M^{j+1}, \qquad 0 \leq j < m. \tag{17}$$

We will now define a group isomorphism σ_r of $A(r)$ into A by setting

$$\sigma_r(j + p^r \mathbb{Z}) = p^{m-r} j + p^m \mathbb{Z}. \tag{18}$$

Observe that the image of σ_r in A is the ideal M^{m-r} of A. The mapping σ_r is called a decimation. It is not a ring homomorphism since

$$p^{m-r} \sigma_r(ab) = \sigma_r(a)\sigma_r(b), \qquad a, b \in A(r). \tag{19}$$

Under the identification (2), the mapping σ_r becomes

$$\sigma_r(k) = p^{m-r} k, \qquad 0 \leq k < p^r. \tag{20}$$

Denote the restriction of σ_r to $U(r)$ by σ_r^* and observe from (20) that

$$\sigma_r^*(U(r)) = D_{m-r}. \tag{21}$$

Thus σ_r^* is a bijection of $U(r)$ onto D_{m-r}.

Define the mapping π_r of A onto $A(r)$ by the rule

$$\pi_r(j + p^m \mathbb{Z}) \equiv j + p^r \mathbb{Z}. \tag{22}$$

The mapping π_r is usually called a natural mapping. We will call it a periodization. As is well known, π_r is a ring homomorphism of A onto $A(r)$ whose kernel is the ideal M^r. This result can be expressed by

$$0 \to M^r \to A \xrightarrow{\pi_r} A(r) \to 0. \tag{23}$$

Using the identification given in (2), for A and $A(r)$, we can write

$$\pi_r(j + kp^r) = j, \qquad 0 \leq j < p^r, 0 \leq k < p^{m-r}. \tag{24}$$

As j and k run over $0 \le j < p^r$, $0 \le k < p^{m-r}$, we have $j + kp^r$ running over A.

Denote the restriction of π_r to the unit group U by π_r^*. Since π_r is a ring homomorphism of A onto $A(r)$, π_r^* is a group homomorphism of U onto $U(r)$. A direct proof can be given from formula (22). In addition, the kernel of the group homomorphism π_r^* is the subgroup $1 + M^r$ of U. We diagram the result as

$$1 \to 1 + M^r \to U \xrightarrow{\pi_r^*} U(r) \to 1. \tag{25}$$

The number of elements in a finite set X will be denoted by $o(X)$ and called the order of X. Then, the order of $U(r)$ is given by

$$o(U(r)) = p^{r-1}(p-1), \tag{26}$$

which we will sometimes denote by t_r.

Since p is an odd prime, the cyclic group U has a generator, say y. The element $z \equiv \pi_r^*(y)$ generates $U(r)$. Since $z^{t_r} = 1$, we have $y^{t_r} \in 1 + M^r$, by (25).

The set D_{m-r} can be described in terms of the generator y of U. From (21),

$$D_{m-r} = \{\sigma_r^*(z^k) : 0 \le k < t_r\}. \tag{27}$$

Since $\sigma_r^*(z^k) = p^{m-r}y^k$, we have

$$D_{m-r} = \{p^{m-r}y^i : 0 \le k < t_r\}. \tag{28}$$

Indeed, every $a \in D_{m-r}$ can be written uniquely in the form

$$a = p^{m-r}y^k, \qquad 0 \le k < t_r. \tag{29}$$

2. Winograd's Canonical Form

Consider the $n \times n$ Fourier transform matrix

$$F(n) = [w^{jk}]_{0 \le j,\, k < n}, \qquad w = \exp(2\pi i/n). \tag{1}$$

If $a \in \mathbb{Z}/n$, then w^a is well defined by the formula

$$w^a \equiv w^j, \qquad a = j + n\mathbb{Z}. \tag{2}$$

We can write (1) as

$$F(n) = [w^{ab}]_{a,\, b \in \mathbb{Z}/n}. \tag{3}$$

Let π be a permutation of $\mathbb{Z}/n$. Define

$$F_\pi(n) \equiv [w^{\pi(a)\pi(b)}]_{a,b\in\mathbb{Z}/n}. \tag{4}$$

There exists a permutation matrix P_π such that

$$(P_\pi)^{-1}F_\pi(n)P_\pi = F(n). \tag{5}$$

If e_j is the n-tuple consisting of all 0's except in the jth place here it has 1, then permutation matrix P_π is given by

$$P_\pi e_j \equiv e_{\pi(j)}, \qquad 0 \le j < n. \tag{6}$$

Take a prime p and an integer $m \ge 1$. Set $n = p^m$. The notation of the preceding section will be continued. Thus, $A = \mathbb{Z}/n$ and U is the unit group of A. The first step in Winograd's algorithm for $n = p^m$ involves defining a permutation π of A such that the matrix $F_\pi(n)$ has a special form, which we call the Winograd canonical form of $F(n)$. We will derive the canonical form in this section. The complete Winograd algorithm can be found in [4].

The ring structure of A, especially the set of U-orbits, will be used to define the permutation π. The resulting $F_\pi(n)$ will be made up of matrix blocks, each of which is a skew-circulant matrix.

Consider the partition of A given by the set of U-orbits

$$U, pU, \ldots, p^mU. \tag{7}$$

We order the set of U-orbits as shown in (7). Assume p is an odd prime. The unit group U is a cyclic group. Take a generator x of U. The elements of each U-orbit will be ordered by the powers of x. The U-orbit

$$D_j = p^jU \tag{8}$$

is ordered as

$$p^jx^0, p^jx^1, \ldots, p^jx^t, \qquad t = o(U(m-j)). \tag{9}$$

Note that we have used (29) of Section 1.

Let π be the permutation of A determined by the ordering of A given by (7) and (9). The set A with this ordering will be denoted by A'. Then,

$$F_\pi(n) = [w^{ab}]_{a,b\in A'}. \tag{10}$$

For $0 \le r, s \le m$, define the $t_{m-r} \times t_{m-s}$ matrix $X(r, s)$ by setting

$$X(r, s) \equiv [w^{ab}], \qquad a \in D_r, b \in D_s. \tag{11}$$

We order D_r and D_s by (9). By (10), we have

$$F_\pi(n) = [X(r,s)]_{0\le r,s\le m}. \tag{12}$$

We will require an additional notation. Let

$$w_j \equiv \exp(2\pi i/n_j), \qquad n_j = p^j. \tag{13}$$

By (2), if $a \in A(j) = \mathbf{Z}/p^j$, then w_j^a is well defined. For notational convenience we set

$$w_j(a) \equiv w_j^a, \qquad a \in A(j). \tag{14}$$

Consider the generator x of U and set

$$x_j \equiv \pi_j^*(x). \tag{15}$$

Then x_j generates $U(j)$ and we have

$$w_j(p^{m-j}x^k) = w_j(x_j^k). \tag{16}$$

The matrices $X(r,s)$, $0 \le r, s \le m$, will be shown to have a special form. The matrices $X(r)$, $0 \le r \le m$, defined below, will be the basic building blocks.

Let $X(m)$ denote the $t \times t$ matrix, $t = o(U)$, given by

$$X(m) = [w(x^{j+k})]_{0\le j,k<t}. \tag{17}$$

Recall, $w = \exp(2\pi i/n)$, $n = p^m$. We call $X(m)$ the core matrix associated to n and the generator x of U. For $0 \le r < m$, we denote by $X(r)$ the core matrix associated to $n_r = p^r$ and the generator $x_r = \pi_r^*(x)$ of $U(r)$.

Since $x^t = 1$, we have $w(x^t) = w$, and, more generally, $w(x^{j+k}) = w(x^r)$ where $r \equiv j + k \bmod t$. It follows from inspection that $x(m)$ is the skew-circulant matrix,

$$X(m) = \begin{bmatrix} w(1) & w(x) & \cdots & w(x^{t-1}) \\ w(x) & & & w(1) \\ w(x^{t-1}) & w(1) & & w(x^{t-2}) \end{bmatrix}. \tag{18}$$

It follows that each matrix $X(r)$, $0 \le r \le m$, is a skew-circulant matrix.

An important part of Winograd's theory is the ability to transform the problem of computing $F(n)v$ into a problem involving circulant matrix multiplication which can then be handled by a polynomial multiplication algorithm. We will not pursue the details, but will show how circulant matrices arise from the skew-circulant matrices $X(r)$, $0 \le r \le m$. It suffices to do this for $r = m$.

Let P be the $t \times t$ permutation matrix given by

$$P = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & 1 \\ 0 & 1 & \cdots & 0 \end{bmatrix}. \tag{19}$$

Note that $P = (1/t)F(t)^2$. A direct computation shows that $PX(m)$ is the circulant matrix

$$PX(m) = \begin{bmatrix} w(1) & w(x) & \cdots & w(x^{t-1}), \\ w(x^{t-1}) & w(1) & & w(x^{t-2}) \\ w(x) & w(x^2) & & w(1) \end{bmatrix}. \tag{20}$$

We will now show that the matrix $X(r, s)$, $0 \le r, s \le m$, is built in a simple manner from the skew-circulant matrix $X(r)$, $0 \le r \le m$. From (11), we recall that

$$X(r, s) = [w(ab)], \qquad a \in D_r, b \in D_s. \tag{21}$$

Using (29) of Section 1, we write $a = p^r x^j$, $0 \le j < t_{m-r}$, and $b = p^s x^k$, $0 \le k < t_{m-1}$. We consider two cases. If $r + s \ge m$ then $ab = p^{r+s}x^{j+k}$ implies $w(ab) = 1$. For integers $u, v > 0$, let $I(u, v)$ denote the $u \times v$ matrix having all coefficients 1. We have just proved that if $r + s \ge m$, then

$$X(r, s) = I(t_{m-r}, t_{m-s}), \qquad t_r = o(U(r)). \tag{22}$$

Suppose now that $r + s < m$. By (16), we have

$$w(ab) = w_v(x_v^{j+k}), \qquad v = m - (r + s), \tag{23}$$

and we write (21) as

$$X(r, s) = \left[w_v(x_v^{j+k})\right]_{0 \le j < t_{m-r}, 0 \le k < t_{m-r}}. \tag{24}$$

The $t_v \times t_v$ matrix formed from the first t_v rows and the first t_v columns of $X(r, s)$ can be seen from (24) to be $X(v)$.

We now use $(x_v)^{t_v} = 1$ to see that the matrix block $X(v)$ is repeated throughout $X(r, s)$. Indeed, we have

$$X(r, s) = I(p^s, p^r) \otimes X(v), \qquad v = m - (r + s) > 0. \tag{25}$$

Combining (12) and (25), we have that $F_\pi(n)$ consists of matrix blocks, each of which is a skew-circulant matrix $X(v)$, $0 \le v \le m$.

We summarize this discussion by the next theorem. Let π be the permutation of A given by (7) and (9) and $P = P_\pi$ the corresponding

matrix given by (6). Define w_v as in (13) and set

$$X(v) = w_v\left(x_v^{j+k}\right), \qquad 0 \le j, k < t_v = o(U(v)).$$

THEOREM. $(P_\pi)^{-1}F(n)P_\pi \equiv F_\pi(n) = [X(r,s)]_{0 \le r,s \le m}$, *where*

1. $X(r,s) = I(t_{m-r}, t_{m-s})$, $t_r = o(U(r))$, *whenever* $r + s \ge m$;

2. $X(r,s) = I(p^s, p^r) \otimes X(v)$, *whenever* $r + s < m$ *and* $v = m - (r+s)$.

3. Periodic and Decimated Data

The viewpoint changes in this section. The Fourier transform F_A of the group $A \equiv \mathbb{Z}/n$ will be defined as a linear operator of complex n-space. Relative to the standard basis, the matrix of F_A will be $F(n)$.

Take $n = p^m$, as before. A bilinear pairing of the ring A will be defined. The Fourier transform F_A is then defined in terms of the bilinear pairing. Although our definition of F_A is standard, the fundamental role of the bilinear pairing in Fourier transform theory is often neglected.

Take $m > 1$. The bilinear pairing establishes a duality between the ideals of A. On the function theoretic level, the ideals of A lead to the concept of periodic and decimated functions. Theorems 1 and 2 give the important implications of duality to the Fourier transform theorem.

This discussion leads to an F_A-invariant subspace, denoted below by $L(1, m-1)$. In Theorem 3 we show that the restriction of F_A to this subspace has a matrix representation given by $pF(p^{m-2})$. This gives an important induction step in our analysis of F_A.

Let S be any finite set of order n. Denote by $L(S)$ the space of all complex-valued functions on S. Under the usual rules of scalar multiplication and addition of functions, $L(S)$ is an n-dimensional complex vector space. In fact, the functions $e_s \in L(S)$, $s \in S$, given by

$$e_s(t) = \begin{cases} 1, & t = s,\ t \in S, \\ 0, & t \ne s,\ t \in S, \end{cases} \tag{1}$$

determine a basis of $L(S)$. We call the basis

$$\{e_s : s \in S\}$$

the standard basis of $L(S)$. Observe that if $f \in L(S)$ then we have

$$f = \sum_{s \in S} f(s) e_s. \tag{2}$$

Consider the ring $A = \mathbb{Z}/n$, $n = p^m$. Denote by $\mathbb{C}^x(1)$, the group of complex numbers of absolute value 1. Let $w = \exp(2\pi i/n)$. Define the mapping

$$\langle\ ,\ \rangle\colon A \times A \to \mathbb{C}^x(1) \tag{3}$$

by setting

$$\langle a, b\rangle \equiv w^{ab}, \qquad a, b \in A, \tag{4}$$

and observe that the following two conditions are satisfied:

$$\begin{aligned} &1.\ \langle a, b\rangle = \langle b, a\rangle, && a, b \in A, \\ &2.\ \langle a + a', b\rangle = \langle a, b\rangle\langle a', b\rangle, && a, a', b \in A. \end{aligned} \tag{5}$$

The mapping (3) is called the bilinear pairing of the ring A.

The theory of the Fourier transform of A and, as we will see, the underlying structure of the algorithms for computing $F(n)v$, discussed in this work, can be developed from the bilinear pairing of A and the concepts arising from the bilinear pairing of A.

The Fourier transform of A, denoted by F_A, is the mapping of $L(A)$ given by

$$F_A(f)(b) \equiv \sum_{a \in A} f(a)\langle a, b\rangle, \qquad f \in L(A), b \in A. \tag{6}$$

A direct computation shows that F_A is a linear transformation of $L(A)$.

By (6), we have

$$F_A(e_a)(b) = \langle a, b\rangle, \qquad a, b \in A. \tag{7}$$

By (2), we then have

$$F_A(e_a) = \sum_{b \in A} \langle a, b\rangle e_b, \qquad a \in A. \tag{8}$$

It follows that the matrix of F_A relative to the basis (1) of $L(A)$ is

$$F(n) = [w^{ab}]_{a, b \in A} = [\langle a, b\rangle]_{a, b \in A}. \tag{9}$$

Assume, for the rest of this section, that $m > 1$.

For any subset B of A, we define the dual $B^\perp$ of B by setting

$$B^\perp \equiv \{a \in A\colon \langle a, b\rangle = 1, \text{ all } b \in B\}. \tag{10}$$

The set $B^\perp$ is a subgroup of A.

Consider the ideals M^j, $1 \le j < m$, of A.

LEMMA 1. $(M^j)^\perp = M^{m-j}$, $1 \le j < m$.

Proof. Observe that, for any $b \in A$, $bM^j = 0$ if and only if $b \in M^{m-j}$. Take any $b \in (M^j)^\perp$. By definition, $\langle b, c\rangle = 1$, for all $c \in M^j$. Since $w^{bc} = \langle b, c\rangle = 1$ if and only if $bc = 0$, we have $bM^j = (0)$ and $b \in M^{m-j}$. It follows that $(M^j)^\perp \; M^{m-j}$. Reversing the steps of the preceding argument shows $M^{m-j}\; (M^j)^\perp$, completing the proof of the lemma.

A function $f \in L(A)$ is called M^j-periodic if

$$f(a + b) = f(a), \qquad a \in A, b \in M^j. \tag{11}$$

Denote the set of all M^j-periodic functions in $L(A)$ by $L(0, j)$. A straightforward computation shows that $L(0, j)$ is a subspace of $L(A)$.

For $0 \le k < p^j$, define $E_k^j \in L(A)$ by the rule

$$E_k^j \equiv \begin{cases} 1 & \text{on } k + M^j, \\ 0 & \text{otherwise.} \end{cases} \tag{12}$$

If $f \in L(0, j)$ then we can write

$$f = \sum_{k=0}^{p^j - 1} f(k) E_k^j. \tag{13}$$

As a consequence, the set

$$\left\{ E_k^j : 0 \le k < p^j \right\} \tag{14}$$

is a basis of $L(0, j)$ and the dimension of $L(0, j)$ is p^j.

Consider again the ring homomorphism π_j of A onto $A(j)$. The mapping π_j^* defined by setting

$$\pi_j^*(f) = f \circ \pi_j, \qquad f \in L(A(j)), \tag{15}$$

is a linear transformation of $L(A(j))$ onto $L(A)$. Since, the kernel of π_j is M^j, π_j^* is a linear transformation of $L(A(j))$ onto $L(0, j)$.

Consider the standard basis $\{e_k^j : 0 \le k < p^j\}$ of $L(A(j))$. A direct computation shows that

$$\pi_j^*\left(e_k^j\right) = E_k^j, \qquad 0 \le k < p^j, \tag{16}$$

which implies that π_j^* is a linear isomorphism of $L(A(j))$ onto $L(0, j)$.

The linear isomorphism π_j^* can also be defined as follows. If $f' \in L(A(j))$ is given by the p^j-tuple

$$f' = \left[f'(0), \ldots, f'\left(p^j - 1\right)\right] \tag{17}$$

then $f = \pi_j^*(f')$ is given by f' repeated p^{m-j} times.

A function $f \in L(A)$ is called M^j-decimated if f vanishes off M^j. Denote the space of M^j-decimated functions by $L(j, m)$. Observe that $L(j, m)$ is a subspace of $L(A)$. The set

$$\left\{ e_{p^j k} : 0 \leq k < p^{m-j} \right\} \tag{18}$$

is a basis of $L(j, m)$.

The group isomorphism σ_{m-j} of $A(m-j)$ into A induces a linear transformation σ^*_{m-j} of $L(j, m)$ into $L(A(m-j))$ by the rule

$$\sigma^*_{m-j}(f) \equiv f \circ \sigma_{m-j}, \qquad f \in L(j, m). \tag{19}$$

Let $\{e^{m-j}: 0 \leq k < p^{m-j}\}$ be the standard basis of $L(A(m-j))$. A straightforward computation shows that

$$\sigma^*_{m-j}(e_{p^j k}) = e^{m-j}_k, \qquad 0 \leq k < p^{m-j}, \tag{20}$$

implying that σ^*_{m-j} is a linear isomorphism of $L(j, m)$ onto $L(A(m-j))$. Using definitions (2) and (15) from Section 1, we can describe σ^*_{m-j} as follows. If $f \in L(j, m)$, then

$$\sigma^*_{m-j}(f) = f(p^j k), \qquad 0 \leq k < p^{m-j}. \tag{21}$$

The relationship between F_A and the spaces of M^j-periodic and M^j-decimated functions is contained in the next two theorems. We state them without proof. The interested reader should consult [13] for proofs.

THEOREM 1. *If f is an M^j-periodic function in $L(A)$ then $F_A(f)$ is M^{m-j}-decimated.*

Explicitly, let $f = \pi_j^*(f')$, $f' \in L(A(j))$. Then,

$$F_A(f) \circ \sigma_j = p^{m-j} F_{A(j)}(f').$$

THEOREM 2. *If f is an M^j-decimated function in $L(A)$, then $F_A(f)$ is M^{m-j}-periodic.*

Explicitly, let $f' = \sigma^*_{m-j}(f)$. Then

$$F_A(f) = F_{A(m-j)}(f') \circ \pi_{m-j}.$$

From Theorem 1, to compute the Fourier transform $F_A(f)$ of an M^j-periodic function f, we begin by finding $f^* \in L(A(j))$ such that $f = \pi_j^*(f')$ and then compute the Fourier transform $F_{A(j)}(f')$ of f'. $F_A(f)$ vanishes from M^{m-j} and M^{m-j} is given by

$$F_A(f)(p^{m-j}k) = p^{m-j} F_{A(j)}(f')(k), \qquad 0 \leq k < p^j. \tag{22}$$

Take $0 < j \le k \le m$ and denote by $L(j, k)$ the subspace of all $f \in L(A)$ such that f is M^j-decimated and M^k-periodic. Theorems 1 and 2 imply

$$F_A(L(j, k)) = L(m - k, m - j). \tag{23}$$

As a special case, we have that

$$F_A(L(1, m - 1)) = L(1, m - 1). \tag{24}$$

Define $E_k \in L(A)$, $0 \le k < p^{m-1}$, by setting

$$E_k \equiv \begin{cases} 1 & \text{on } k + M^{m-1}, \\ 0 & \text{otherwise.} \end{cases} \tag{25}$$

Compare (25) with (12). The set

$$\{E_{pk} : 0 \le k < p^{m-2}\} \tag{26}$$

is a basis of $L(1, m - 1)$. In fact, if $f \in L(1, m - 1)$ then

$$f = \sum_{j=0}^{p^{m-2}} f(pj) E_{pj}. \tag{27}$$

THEOREM 3. *The matrix of F_A restricted to $L(1, m - 1)$ relative to the basis* (26) *is $pF(p^{m-2})$.*

Proof. Since $F_A(E_{pk}) \in L(1, m - 1)$, $0 \le k < p^{m-2}$, we can write

$$F_A(E_{pk}) = \sum_{j=0}^{p^{m-2}-1} F_A(E_{pk})(pj) E_{pj}.$$

By definition, where $w = \exp(2\pi i/n)$, $n = p^m$, we have

$$F_A(E_{pk})(pj) = \sum_{u=0}^{n-1} E_{pk}(u) w^{upj}, \qquad 0 \le j < p^{m-2},$$

which by (25) becomes

$$F_A(E_{pk})(pj) = \sum_{v=0}^{p-1} w^{(pk+p^{m-1}v)pj} = pv^{kj},$$

where $v = \exp(2\pi i/p^{m-2})$. It follows that

$$F_A(E_{pk}) = p \sum_{j=0}^{p^{m-2}-1} v^{jk} E_{pj}, \qquad 0 \le k < p^{m-2},$$

completing the proof of the theorem.

4. Multiplicative Characters

For $m > 1$, the F_A-invariant subspace $L(1, m-1)$ has an F_A-invariant orthogonal complement in $L(A)$, denoted by C. Then we can study the action of F_A on each of the factors of the orthogonal direct sum decomposition

$$L(A) = C \oplus L(1, m-1). \tag{1}$$

The multiplicative characters of A, defined below, provide the main tool for studying the action of F_A on C. A basis for C will be constructed from the multiplicative characters and their Fourier transform. The power of multiplicative characters as a Fourier analysis tool will be seen in the next section when explicit formulas describing the Fourier transform of multiplicative characters are derived.

For any finite set S, we make $L(S)$ into an inner product by setting

$$\langle f, g \rangle \equiv \sum_{j \in S} f(j) g^*(j), \qquad f, g \in L(S). \tag{2}$$

As usual * denotes the complex conjugation.

Consider the standard basis $\{e_a;\ a \in A\}$ of $L(A)$, where $A = \mathbb{Z}/n$, $n = p^m$. Applying definition (2),

$$\langle e_a, e_b \rangle = \begin{cases} 1, & a = b;\ a, b \in A, \\ 0, & a \neq b;\ a, b \in A, \end{cases} \tag{3}$$

implying that the standard basis is an orthonormal basis.

We will show that $n^{-1/2}F_A$ is a unitary operator. Recall, $w = \exp(2\pi i/n)$. Then

$$\sum_{b \in A} w^{ab} = \begin{cases} n & a = 0;\ a \in A, \\ 0 & a \neq 0;\ a \in A. \end{cases} \tag{4}$$

Take $a, b \in A$. By (7) of Section 3, we have

$$\langle F_A e_a, F_A e_b \rangle = \sum_{c \in A} \langle a, c \rangle \langle c, b \rangle^* = \sum_{c \in A} w^{c(a-b)} = \begin{cases} n, & a = b, \\ 0, & a \neq b. \end{cases} \tag{5}$$

It follows that $n^{-1/2}F_A$ is is a unitary operator.

Take $m > 1$. The orthogonal complement C of $L(1, m-1)$ in $L(A)$ is defined by

$$C \equiv \{ f \in L(A);\ \langle f, g \rangle = 0 \qquad \text{for all } g \in L(1, m-1) \}. \tag{6}$$

From general theory, C is an F_A-invariant subspace and

$$L(A) = C \oplus L(1, m-1). \tag{7}$$

We will study the action of F_A on the subspace C in the next section. We introduce the main tool of the study, the multiplicative characters of the ring A, at this time. A mapping

$$\lambda: U \to \mathbb{C}^x(1) \tag{8}$$

is called a multiplicative character of A, if

$$\lambda(uv) = \lambda(u)\lambda(v), \qquad u, v \in U. \tag{9}$$

$\mathbb{C}^x(1)$ is the group of complex numbers of absolute value 1. Equivalently, a multiplicative character of A is a group homomorphism of U onto $\mathbb{C}^x(1)$. We have

$$\lambda(1) = 1 \qquad \text{and} \qquad \lambda(u^{-1}) = (\lambda(u))^{-1} = \lambda^*(u),\ u \in U. \tag{10}$$

The group U has t elements where

$$t = \begin{cases} p-1, & m = 1, \\ (p-1)p^{m-1}, & m > 1. \end{cases} \tag{11}$$

Thus, $u \in U$ implies $u^t = 1$. Let λ be a multiplicative character of A. Then, $\lambda(u)^t = \lambda(u^t) = \lambda(1) = 1$ and $\lambda(u)$ is a tth root of unity. Denote the multiplicative group of all complex tth roots of unity by $U_n(t)$. Let

$$v = \exp(2\pi i/t) \tag{12}$$

in all that follows. The complex number v generates the cyclic group $U_n(t)$. Since the multiplicative character λ of A is a group homomorphism, $\lambda(U)$ is a subgroup of $U_n(t)$.

Denote by $\hat{U}$ the set of all multiplicative characters of A. $\hat{U}$ becomes a group under the product and inverse rules

$$\begin{aligned} (\lambda\lambda')(u) &\equiv \lambda(u)\lambda'(u) \\ \lambda^{-1}(u) &\equiv (\lambda(u))^{-1} = \lambda^*(u), \qquad u \in U,\ \lambda, \lambda' \in \hat{U}. \end{aligned} \tag{13}$$

The identity element of $\hat{U}$ is given by

$$\lambda_0(u) \equiv 1, \qquad u \in U. \tag{14}$$

Since we are assuming p is an odd prime, the group U has a generator, say y. We will denote the order U by t. We will now prove that $\hat{U}$ is a cyclic group of order t. For any k, $0 \le k < t$, define the mapping λ_k; $U \to U_n(t)$ by setting

$$\lambda_k(y^j) \equiv v^{kj}, \qquad 0 \le j < t, \qquad v = \exp(2\pi i/t). \tag{15}$$

A straightforward computation shows that λ_k is a multiplicative character of A. Moreover, if $\lambda \in \hat{U}$ then $\lambda(y) = v^k$ for some $0 \le k < t$. By definition (9), $\lambda = \lambda_k$.

LEMMA 1. *$\hat{U}$ is a cyclic group of order t.*

Proof. The preceeding discussion implies

$$\hat{U} = \{\lambda_k : 0 \le k < t\}.$$

Since $\lambda_k = \lambda_1^k$, the lemma is proved with λ_1 as a generator of $\hat{U}$.

Extend the domain of definition of each $\lambda \in \hat{U}$ to all of A by setting $\lambda(a) = 0$ whenever $a \in M = A - U$. In this way, we will always assume $\hat{U} \subset L(A)$.

Take $m > 1$ on all that follows. Denote by $\hat{U}_j$ the set of all M^j-periodic multiplicative characters of A. Observe that $\hat{U}_j$ is a subgroup of $\hat{U}$ and we have

$$\phi = \hat{U}_0 \subset \hat{U}_1 \subset \cdots \subset \hat{U}_{m-1} \subset \hat{U}_m = \hat{U}. \tag{16}$$

Recall the linear isomorphism π_j^* of $L(A(j))$ onto the space $L(0, j)$ of M^j-periodic functions on $L(A)$. If π_j is the ring homomorphism of A onto $A(j)$ defined in (1.22), then $\pi_j^*(f) = f \circ \pi_j$.

Take any multiplicative character λ' of $A(j)$. The set of all multiplicative characters of $A(j)$ will be denoted by $\hat{U}(j)$. Since π_j restricts to a group homomorphism of U onto $U(j)$,

$$\lambda \equiv \pi_j^*(\lambda') \tag{17}$$

is a multiplicative character of A, implying $\lambda \in \hat{U}_j$. The restriction of π_j^* to $\hat{U}(j)$ is a group isomorphism of $\hat{U}(j)$ onto $\hat{U}_j$.

LEMMA 2. *π_j^* restricts to a group isomorphism of $\hat{U}(j)$ onto $\hat{U}_j$.*

Proof. We must prove onto. Take any $\lambda \in \hat{U}_j$ and write $\lambda \equiv_j^* (\lambda')$, where $\lambda' \in L(A(j))$. We will show $\lambda' \in \hat{U}(j)$. Take $a', b' \in U(j)$ and write $a' = \pi_j(a)$, $b' = \pi_j(b)$, for some $a, b \in U$. Then $\pi_j(ab) = \pi_j(a)\pi_j(b) = a'b'$ and

$$\lambda'(a'b') = \lambda'\big(\pi_j(ab)\big) = \lambda(ab) = \lambda(a)\lambda(b) = \lambda'(a')\lambda'(b'),$$

proving the lemma.

Form the set differences

$$V_j \equiv \hat{U}_j - \hat{U}_{j-1}, \qquad 1 \le j \le m. \tag{18}$$

The collection of sets

$$\{V_j : 1 \le j \le m\} \tag{19}$$

is a partition of $\hat{U}$.

The elements in V_m are called primitive multiplicative characters of A. They play a special role in our theory. The elements in W_m,

$$W_m = \hat{U} - V_m \tag{20}$$

are called non-primitive multiplicative characters of A. By Lemma 2,

$$o(V_m) = o(U) - o(U(m-1)) = (p-1)^2 p^{m-2}.$$

In general,

$$o(V_j) = o(U(j)) - o(U(j-1) = (p-1)^2 p^{j-2}, \qquad j \geq 2, \tag{21}$$

and

$$o(V_1) = p - 1. \tag{22}$$

Denote the set of all primitive multiplicative characters of $A(j)$ by $V(j)$. We take $V(1) \equiv \hat{U}(1)$.

LEMMA 3. *π_j^* maps $V(j)$ bijectively onto V_j.*

Proof. Since $o(V(j)) = o(V_j)$, we are done once we show $\pi_j^*(V(j))V_j$. Take $\lambda' \in V(j)$. For some $a' \in A(j)$ and $b' \in p^{j-1}A(j)$, we have

$$\lambda'(a' + b') \equiv \lambda'(a').$$

Since π_j maps A onto $A(j)$ and M^{j-1} onto $p^{j-1}A(j)$, we can write

$$a' = \pi_j(a), \qquad b' = \pi_j(b), \qquad a \in A,\ b \in M^{j-1}.$$

Let $\lambda \equiv \pi_j^*(\lambda')$. Then

$$\lambda(a+b) = \lambda'(a' + b') \neq \lambda'(a') = \lambda(a),$$

implying $\lambda \notin \hat{U}_{j-1}$ and $\lambda \in V_j$.

By Lemma 1, $\hat{U}$ is the cyclic group generated by λ_1. The subsets V_j of (24) will be characterized relative to the powers of λ_1.

First we determine the powers of λ_1 making up $\hat{U}_{m-1}$. Suppose $\lambda_1^k \in \hat{U}_{m-1}$ and write, by Lemma 2,

$$\lambda_1^k = \lambda' \circ \pi_{m-1}, \qquad \lambda' \in \hat{U}(m-1). \tag{23}$$

Then

$$\lambda_1^k(U) = \lambda'(U(m-1)) \subset U_n(t_{m-1}) \qquad \text{where } t = p^{t_{m-1}}. \tag{24}$$

Since v^p generates $U_n(t_{m-1})$, $v = \exp(2\pi i/t)$, $\lambda_1^k(y) = v^k \in U_n(t_{m-1})$, im-

plying $p|k$. Thus $\lambda_1^k \in \hat{U}_{m-1}, 0 \le k < t$, implies $p|k$. Since $o(\hat{U}_{m-1}) = t_{m-1}$, we have

$$\hat{U}_{m-1} = \left\{(\lambda_1)^{kp} : 0 \le k < t_{m-1}\right\}. \tag{25}$$

This discussion leads to

LEMMA 4. $V_m = V(m) = \{\lambda_1^k : 0 \le k < t, p \nmid k\}$.

More generally, the same argument proves

LEMMA 5. $V_r = \{\lambda_1^{p^{m-r}} : 0 \le k < p^r\}$.

5. FOURIER TRANSFORMS OF MULTIPLICATIVE CHARACTERS

In Section 3, we defined subspaces of $L(A)$ by periodicity and decimation conditions. We begin this section by relating these subspaces to subspaces spanned by sets of multiplicative characters and to subspaces spanned by the Fourier transforms of multiplicative characters. The inner product structure of $L(A)$ will play a major role. The main result of this part determines an orthogonal direct sum decomposition of $L(A)$ having $L(1, m-1)$ as a factor along with subspaces formed from multiplicative characters.

In the second part of this section, we will derive explicit formulas computing the Fourier transforms of multiplicative characters. From these formulas, we determine an important basis of $L(A)$ which is made up, in part, of multiplicative characters and their Fourier transforms.

To begin with, we need a technical result.

LEMMA 1. *Suppose* $m \ge 1$. *For* $\lambda \in \hat{U}$.

$$\sum_{u \in U} \lambda(u) = \begin{cases} t, & \lambda = \lambda_0, t = o(U), \\ 0, & \lambda \ne \lambda_0, t = o(U), \end{cases}$$

(*recall,* λ_0 *is the identity element in* $\hat{U}$).

Proof. If $\lambda = \lambda_0$ then $\lambda(u) = 1$, $u \in U$, and this case of the lemma follows. Suppose $\lambda \ne \lambda_0$. Then there is a $u_0 \in U$ such that $\lambda(u_0) \ne 1$. As u runs over U, uu_0 runs over U. Thus

$$\sum_{u \in U} \lambda(u) = \sum_{u \in U} \lambda(uu_0) = \lambda(u_0) \sum_{u \in U} \lambda(u) = 0,$$

completing the proof of the lemma.

Applying Lemma 1 to the definition of the inner product, the set

$$t^{-1/2}\hat{U} \equiv \{t^{-1/2}\lambda : \lambda \in \hat{U}\} \tag{1}$$

is orthonormal. Since $n^{-1/2}F_A$ is unitary, the set

$$(nt)^{-1/2}F_A(\hat{U}) \tag{2}$$

is orthonormal.

Take $m = 1$ and let $\{e_j\}$ be the standard basis of $L(A(1))$. The set

$$\{e_0\} \cup t^{-1/2}\hat{U} \tag{3}$$

is an orthonormal basis of $L(A(1))$.

Take $m > 1$, until otherwise stated. Define

$$W_m \equiv \hat{U} - V_m. \tag{4}$$

By definition,

$$W_m \subset L(0, m-1). \tag{5}$$

Applying (3.28), we have

$$F_A(W_m) \subset L(1, m). \tag{6}$$

Consider the set

$$\Omega_m \equiv V_m \cup W_m \cup F_A(W_m). \tag{7}$$

THEOREM 1. *Ω_m is an orthogonal set.*

Proof. $V_m \cup W_m = \hat{U}$ is orthogonal by (2). Since $\lambda \in \hat{U}$ vanishes from U and $f \in F_A(W_m)$ vanishes on U, we have $\langle \lambda, f \rangle = 0$, implying $\hat{U}$ is orthogonal to $F_A(W_m)$. Finally, $n^{-1/2}F_A$ being unitary implies orthogonality of $F_A(\hat{U})$. In particular, $F_A(W_m)$ is orthogonal, completing the proof of the theorem.

Consider the subspace $L(1, m-1)$. As we pointed out in Section 3 $L(1, m-1)$ is F_A-invariant. Denote the orthogonal complement of $L(1, m-1)$ in $L(A)$ by C. The dimension of C is $p^m - p^{m-2}$.

THEOREM 2. *The set Ω_m is an orthogonal basis of C.*

Proof. Since the order of Ω_m is $p^m - p^{m-2}$[1], the same as the dimension of C, we must show $\Omega_m C$. Clearly, $\hat{U}$ is orthogonal to $L(1, m-1)$. For $\lambda \in \hat{U}$, $f \in L(1, m-1)$, we have

$$\langle f, F_A(\lambda)\rangle = \langle F_A\big((F_A)^{-1}\big)(f), F_A(\lambda)\rangle.$$

But $L(1, m-1)$ is $(F_A)^{-1}$-invariant and $F_A(f) \in L(1, m-1)$. It follows

that $\langle (F_A)^{-1}f, \lambda \rangle = 0$. Since $n^{-1/2}F_A$ is unitary, we have $\langle f, F_A(\lambda) \rangle = 0$, completing the proof of theorem.

Denote by $\mathrm{Ln}(X)$ the linear span of the subset X of $L(A)$. Theorem 2 leads to the orthogonal direct sum decomposition

$$L(A) = \mathrm{Ln}(\Omega_m) \oplus L(1, m-1). \tag{8}$$

We will examine (8) in greater detail. By (5), (6), and Theorem 2, W_m lies in the orthogonal complement of $L(1, m-1)$ in $L(0, m-1)$ and $F_A(W_m)$ lies in the orthogonal complement of $L(1, m-1)$ in $L(1, m)$. Arguing by dimension, we have the next result.

THEOREM 3. $\mathrm{Ln}(W_m)$ *is the orthogonal complement of* $L(1, m-1)$ *in* $L(0, m-1)$ *and* $\mathrm{Ln}(F_A(W_m))$ *is the orthogonal complement of* $L(1, m-1)$ *in* $L(1, m)$.

We have, by Theorem 3, the orthogonal direct sum decompositions

$$\begin{aligned} L(0, m-1) &= \mathrm{Ln}(W_m) \oplus L(1, m-1) \\ L(1, m) &= \mathrm{Ln}(F_A(W_m)) \oplus L(1, m-1). \end{aligned} \tag{9}$$

It follows from (9) and (8) that $\mathrm{Ln}(W_m) \oplus \mathrm{Ln}(F_A(W_m))$ is the orthogonal complement of $L(1, m-1)$ in $L(0, m-1) + L(1, m)$. Since $L(1, m-1)$ and $L(0, m-1) + L(1, m)$ are F_A-invariant, we have that $\mathrm{Ln}(W_m) \oplus \mathrm{Ln}(F_A(W_m))$ is F_A-invariant. Summarizing, we have the orthogonal direct sum decomposition

$$L(A) = \mathrm{Ln}(V_m) \oplus (\mathrm{Ln}(W_m)) \oplus \mathrm{Ln}(F_A(W_m)) \oplus L(1, m-1) \tag{10}$$

into the F_A-invariant subspaces

$$\mathrm{Ln}(V_m), \qquad \mathrm{Ln}(W_m) \oplus \mathrm{Ln}(F_A(W_m)), \qquad L(1, m-1). \tag{11}$$

Explicit formulas computing the Fourier transforms of multiplicative characters will now be derived. Take $m \geq 1$ and $\lambda \in V(m)$. Denote the identity element in $\hat{U}$ and λ_0. Define

$$G_m(\lambda) \equiv F_A(\lambda)(1) \tag{12}$$

and call $G_m(\lambda)$, the Gauss sum of λ. We begin by studying the case $m = 1$.

LEMMA 2. $F_{A(1)}(\lambda_0) = (p-1)e_0 + (-1)\lambda_0$, $\lambda_0 \in \hat{U}(1)$.

Proof. This follows by a straightforward computation.

LEMMA 3. *If* $\lambda \in \hat{U}(1)$, $\lambda \neq \lambda_0$ *then*

$$F_{A(1)}(\lambda) = G_1(\lambda)\lambda^{-1}.$$

Proof. For $u' \in U$, as u runs over U, we have $u'u$ running over U. It follows that

$$\begin{aligned} F_A(\lambda)(u') &= \sum_{u \in U} \lambda(u) w^{uu'} = \sum_{u \in U} \lambda(uu'^{-1}) w^u, \qquad u' \in U \\ &= \lambda(u'^{-1}) \sum_{u \in U} \lambda(u) w^u \\ &\doteq G_1(\lambda)\lambda^{-1}(u'), \end{aligned}$$

proving the formula on U. The proof of the lemma is completed by observing that $F_A(\lambda)(0) = \sum_{u \in U} \lambda(u) = 0$, by Lemma 1.

Take $m > 1$, until otherwise stated.

LEMMA 4. *If* $\lambda \in V(m)$ *then there is a* $c \in 1 + M^{m-1}$ *such that* $\lambda(c) \neq 1$.

Proof. Suppose $\lambda(1 + M^{m-1}) = 1$. Then, for $u \in U$ and $b \in M^{m-1}$, we have $u^{-1}b \in M^{m-1}$, $1 + u^{-1}b \in 1 + M^{m-1}$, $\lambda(1 + u^{-1}b) = 1$, and

$$\lambda(u + b) = \lambda\big(u(1 + u^{-1}b)\big) = \lambda(u)\lambda(1 + u^{-1}b) = \lambda(u), \quad (13)$$

implying $\lambda \in \hat{U}_{m-1}$, a contradiction.

THEOREM 4. *For* $\lambda \in V(m)$, $m > 1$,

$$F_A(\lambda) = G_m(\lambda)\lambda^{-1}.$$

Proof. If $u' \in U$, then the proof that

$$F_A(\lambda)(u') = G_m(\lambda)\lambda^{-1}(u')$$

proceeds exactly as the corresponding part of Lemma 2.

Take $b \in M = A - U$ and write $b = pb'$, $b' \in A$. Choose $c \in 1 + M^{m-1}$ such that $\lambda(c) \neq 1$. Then $p = pc$ and

$$w^{ub} = w^{pub'} = w^{pub'c} = w^{ubc}.$$

Since $\lambda^{-1}(c) \neq 1$, from

$$F_A(\lambda)(b) = \lambda(c)^{-1} F_A(\lambda)(b),$$

we have $F_A(\lambda)(b) = 0$, completing the proof of the theorem.

Suppose $\lambda \in V_j$ and

$$\lambda = \pi_j^*(\psi), \qquad \psi \in V(j). \tag{14}$$

By Theorem 1, Section 3, $F_A(\lambda)$ is M^{m-j}-decimated and

$$F_A(\lambda) \circ \sigma_j = p^{m-j} F_{A(j)}(\psi), \tag{15}$$

where σ_j is the group isomorphism of $A(j)$ onto M^{m-j} given in (18), Section 1.

Applying Theorem 4 to the computation $F_{A(j)}(\psi)$, where ψ is a primitive multiplicative character of $A(j)$. We have the next result.

THEOREM 5. *If $\lambda \in V_j$ and $\lambda \neq \lambda_0$ then $F_A(\lambda)$ is M^{m-j}-decimated and*

$$F_A(\lambda) \circ \sigma_j = p^{m-j} G_j(\psi) \psi^{-1}, \qquad \lambda = \pi_j^*(\psi).$$

Continue the assumption of Theorem 5. Since ψ vanishes from $U(j)$, $F_A(\lambda)$ vanishes from

$$D_{m-j} \equiv p^{m-j} U. \tag{16}$$

Observe that if $u = \sigma_j(u')$, $u' \in U(j)$ then

$$\lambda(p^{m-j}u) = \psi(u'), \qquad \lambda = \pi_j^*(\psi). \tag{17}$$

This discussion leads to the following corollary of Theorem 5.

COROLLARY. *If $\lambda \in V_j$, $\lambda \neq \lambda_0$, then*

$$F_A(\lambda)(p^{m-j}u) = p^{m-j} G_j(\psi) \lambda^{-1}(u), \qquad u \in U.$$

The same argument proves the next result.

THEOREM 6. *$F_A(\lambda_0)$ is M^{m-1}-decimated and*

$$F_A(\lambda_0)(p^{m-1}k) = \begin{cases} p^{m-1}(p-1), & k = 0, \\ -p^{m-1}, & 0 < k < p. \end{cases}$$

Define $g_{\lambda_0} \in L(m-1, m)$ by setting

$$g_{\lambda_0}(p^{m-1}k) \equiv \begin{cases} -p^{-1/2}(p-1), & k = 0, \\ -p^{-1/2}, & 0 < k < p. \end{cases} \tag{18}$$

Theorem 6 implies

$$F_A(\lambda_0) = -p^{1/2} p^{m-1} g_{\lambda_0}. \tag{19}$$

For $\lambda \in V_j$, $\lambda \neq \lambda_0$, define $g_\lambda \in L(m-j, m)$ by setting

$$g_\lambda(p^{m-j}u) \equiv \lambda^{-1}(u), \qquad u \in U, \tag{20}$$

which, by the corollary to Theorem 5, satisfies

$$F_A(\lambda) = p^{m-j}G_j(\psi)g_\lambda, \qquad \lambda = \pi_j^*(\psi). \tag{21}$$

Let $t_\lambda \equiv t_j = o(u(j))$ whenever $\lambda \in V_j$. A straightforward computation from (18) and (20) implies

$$t_\lambda = \langle g_\lambda, g_\lambda \rangle, \qquad \lambda \in V_j. \tag{22}$$

From Theorem 1, we have the next result.

THEOREM 7. *The set*

$$t^{-1/2}V_m \cup t^{-1/2}W_m \cup \left\{(t_\lambda)^{-1/2}g_\lambda : \lambda \in W_m\right\}$$

is an orthonormal basis of the orthogonal complement C of $L(1, m-1)$ *in* $L(A)$.

6. RATIONAL SUBSPACES

Multiplicative character theory provides a natural setting for developing the complexity results of Auslander, Feig, and Winograd. The first reason for this is the simplicity of the formula describing the action of the Fourier transform on multiplicative characters. We will now discuss a second important property of multiplicative characters. In the sense defined below, the spaces V_j, $1 \leq j \leq m$, as well as the associated spaces of Fourier transforms are rational subspaces. As a consequences, we will be able to "rationally" manipulate the Fourier transform matrix $F(p^m)$ into block diagonal matrices, where each block corresponds to a polynomial multiplication in an appropriate polynomial ring modulo a rational polynomial, in a straightforward fashion. The Chinese remainder theorem will be used at this point.

A function $f \in L(A)$ is called a rational vector if f lies in the rational linear span of the standard basis of $L(A)$. A subspace X of $L(A)$ is called a rational subspace if X has a basis consisting solely of rational vectors. Such a basis will be called a rational basis of X.

Suppose $m = 1$. Consider the set

$$V' \equiv \hat{U} - \{\lambda_0\}. \tag{1}$$

We will construct a rational basis for $\mathrm{Ln}(V')$.

Let y be a generator of U. Define $r_j \in L(A)$, $0 \le j < p-2$, by setting

$$r_j \equiv e_{y^j} - e_{y^{p-2}}. \tag{2}$$

The set

$$R(1) \equiv \{r_j : 0 \le j < p-2\} \tag{3}$$

consists of rational vectors.

THEOREM 1. *Let $m = 1$. The set $R(1)$ is a rational basis of $\mathrm{Ln}(V')$. For each $\lambda \in V'$, we have*

$$\lambda = \sum_{j=0}^{p-3} \lambda(y^j) r_j. \tag{4}$$

Proof. It suffices to prove (4). By definition, formula (4) holds at the powers y^j, $0 \le j < p-2$. We need to show that $\lambda \in V'$ implies

$$\lambda(y^{p-2}) = \sum_{j=0}^{p-3} \lambda(y^j) r_j(y^{p-2}).$$

By definition,

$$\sum_{j=0}^{p-3} \lambda(y^j) r_j(y^{p-2}) = -\sum_{j=0}^{p-3} (y^j).$$

Since $\lambda \neq \lambda_0$, $\sum_{j=0}^{p-2} \lambda(y^j) = 0$, implying

$$\sum_{j=0}^{p-3} \lambda(y^j) r_j(y^{p-2}) = \lambda(y^{p-2})$$

and completing the proof of the theorem.

The set V' is given by

$$V' = \{\lambda_k : 1 \le k < p-1\}, \tag{5}$$

where $\lambda_k(y_j) \equiv (v_1)^{jk}$, $v_1 = \exp(2\pi i/p-1)$. It follows that the matrix

$$X(1) \equiv \left[(v_1)^{jk}\right], \qquad 0 \le j < p-2, 0 < k < p-1, \tag{6}$$

where $v_1 = \exp(2\pi i/p-1)$, is the change of basis matrix taking $R(1)$ onto V'.

Take $m > 1$. We will show that $\mathrm{Ln}(V(m))$ is a rational subspace of $L(A)$. Denote a generator of U by y. Define $r_j \in L(A)$, $0 \le j < s = o(V(m))$, by the rule

$$r_j \equiv e_{y^j} + r_j', \tag{7}$$

where r_j', $0 \le j < s$, is defined as follows. Let $t = o(U)$ and

$$\alpha \equiv (p-1)p^{m-2} = t - s. \tag{8}$$

Each j, $0 \le j < s$, can be written uniquely in the form

$$j = a + b, \qquad 0 \le a < \alpha, 0 \le b < p-1. \tag{9}$$

Define

$$r_j' \equiv -e_{y^{s+a}}, \qquad j = a + b\alpha, 0 \le a < \alpha, 0 \le b < p-1. \tag{10}$$

The set

$$R(m) \equiv \{r_j : 0 \le j < s\} \tag{11}$$

consists of rational vectors.

THEOREM 2. *Let $m > 1$. The set $R(m)$ is a rational basis of* $\mathrm{Ln}(V(m))$. *If $\lambda \in V(m)$ then*

$$\lambda = \sum_{j=0}^{s-1} \lambda(y^j) r_j. \tag{12}$$

Proof. It suffices to prove (12). By definitions (7) and (10), formula (12) holds at the powers y^j, $0 \le j < s$. We must show that formula (12) continues to hold at the powers y^k, $s \le k < t$. Take k, $s \le k < t$ and write $k = s + a$. We have $0 \le a < \alpha$. Then,

$$r_j(y^k) = r_j'(y^k) = \begin{cases} -1, & j = a + b\alpha, 0 \le b < p-1, \\ 1 & \text{otherwise,} \end{cases}$$

and we have

$$\sum_{j=0}^{s-1} \lambda(y^j) r_j(y^k) = -\sum_{b=0}^{p-2} \lambda(y^{a+b\alpha}) = -\lambda(y^a) \sum_{b=0}^{p-2} \lambda(y^{b\alpha}).$$

Note that $t = p\alpha$ and $(y^{bp\alpha}) = 1$. Since $\lambda \in V(m)$, $\lambda(\lambda^\alpha) \ne 1$ and we have

$$\sum_{b=0}^{p-1} \lambda(y^{b\alpha}) = 0.$$

As a consequence,

$$\sum_{j=0}^{s-1} \lambda(y^j) r_j(y^k) = \lambda(y^a)\lambda(y^{(p-1)\alpha}) = \lambda(y^{a+s}) = \lambda(y^k),$$

completing the proof of the theorem.

The set $V(m)$ is given by

$$V(m) = \{\lambda_k : 0 \le k < t,\ p \nmid k\}, \tag{13}$$

where $\lambda_k(y^j) = (v_m)^{jk}$, $v_m = \exp(2\pi i/t)$. It follows that the matrix

$$X(m) \equiv \left[(v_m)^{jk}\right], \qquad 0 \le j < s, 0 \le k < t,\ p \nmid k, \tag{14}$$

where $t = o(U)$, $s = o(V(m))$, and $v_m = \exp(2\pi i/t)$ is the change of basis matrix taking $R(m)$ onto $V(m)$.

Taking $m > 1$ and $1 \le j < m$. By definition,

$$\mathrm{Ln}(V(j)) = L(0, j). \tag{15}$$

Consider again the linear isomorphism π_j^* of $L(A(j))$ onto $L(0, j)$. The linear isomorphism π_j^* maps the standard basis of $L(A(j))$ onto the standard basis ((18), Sect. 3) of $L(0, j)$. Observe that any rational linear combination of the rational basis ((18), Sect. 3) is a rational vector in $L(A)$.

Suppose $j = 1$. Let

$$V_1' \equiv V - \{\lambda_0\}. \tag{16}$$

By Lemma 3 of Section 4, π_1^* bijectively maps V' onto V_1'. Applying Theorem 1 to the subspace $\mathrm{Ln}(V')$ of $L(A(1))$, we construct the rational basis $R(1)$ of $\mathrm{Ln}(V')$ satisfying (5). Then,

$$R^1(m) \equiv \pi_j^*(R(1)) \tag{17}$$

is a rational basis of $\mathrm{Ln}(V_1')$. Set

$$r_k^1 \equiv \pi_1^*(r_k), \qquad r_k \in R(1), 0 \le k < p - 2. \tag{18}$$

Let y be a generator of U. Using (5), we have the next result.

THEOREM 3. *Let $m > 1$. If $\lambda \in V_1'$ then*

$$\lambda = \sum_{j=0}^{p-3} \lambda(y^j) r_j^1. \tag{19}$$

The change of basis matrix taking $R^1(m)$ onto V_1' is $X(1)$.

Suppose now $m > 2$ and $1 < j < m$. Applying Theorem 2 to the subspace $\mathrm{Ln}(V(j))$ of $L(A(j))$, we construct the rational basis $R(j)$ of $\mathrm{Ln}(V(j))$ satisfying (14). Then,

$$R^j(m) \equiv \pi_j^*(R(j)) \tag{20}$$

is a rational basis of $\mathrm{Ln}(V_j)$. Set

$$r_k^j \equiv \pi_j^*(r_k), \qquad r_k \in R(j), \qquad 0 \le k < s_j = o(V(j)). \tag{21}$$

From (14), we get

THEOREM 4. *If $m > 2$ and $1 < j < m$, then for each $\lambda \in V_j$, we have*

$$\lambda = \sum_{k=0}^{s_j - 1} \lambda(y^k) r_k^j. \tag{22}$$

The change of basis matrix taking $R^j(m)$ onto V_j is $X(j)$.

We will now show that the subspaces $\mathrm{Ln}(F_A(V_j))$ are rational subspaces. First observe that

$$\mathrm{Ln}\big(F_A(V_j)\big) \subset L(m-j, m). \tag{23}$$

The linear isomorphism σ_j^* of $L(m-j, m)$ onto $L(A(j))$ maps the rational basis ((23), Sect. 3) of $L(m-j, m)$ onto the standard basis of $L(A(j))$. Consider the basis ((20), Sect. 5)

$$\{g_{\lambda^{-1}}: \lambda \in V_j\} \tag{24}$$

of $\mathrm{Ln}(F_A(V_j))$. The linear isomorphism σ_j^* maps the basis (24) onto the basis $V(j)$. We can now argue as above to prove the next two results.

THEOREM 5. *There is a rational basis*

$$S^1(m) \equiv \{R_k^1: 0 \le k < p-2\}$$

of $\mathrm{Ln}(F_A(V_1'))$ *such that if* $\lambda \in V_1'$ *then*

$$g_{\lambda^{-1}} = \sum_{k=0}^{p-3} \lambda(y^k) R_k^1. \tag{25}$$

Observe that the change of basis matrix taking $S^1(m)$ onto $\{(g_\lambda)^{-1}: \lambda \in V_1'\}$ is $X(1)$.

THEOREM 6. *If $m > 2$ and $1 < j < m$ then there is a rational basis*

$$S^j(m) \equiv \{R_k^j: 0 \le k < s_j\}, \qquad s_j = o(V_j)$$

of $\mathrm{Ln}(F_A(V_j))$ *such that* $\lambda \in V_j$ *implies*

$$g_{\lambda^{-1}} = \sum_{k=0}^{s_j^{-1}} \lambda(y^k) R_k^j. \tag{26}$$

The change of basis matrix is $X(j)$.

Observe that λ_0 and $p^{-1/2}g$ are rational vectors. Thus, $\mathrm{Ln}(\{\lambda_0, g_\lambda\})$ is a rational subspace and $\{\lambda_0, p^{1/2}g_{\lambda_0}\}$ is a rational basis. The basis $\{E_{pk}: 0 \le k < p^{m-2}\}$ of $L(1, m-1)$ is a rational basis. By (10) of Section 5, if $m = 2$ then $L(A(2))$ is the orthogonal direct sum of the rational subspaces

$$\mathrm{Ln}(V_2), \quad \mathrm{Ln}(V_1'), \quad \mathrm{Ln}(F_A(V_1')), \quad \mathrm{Ln}\left(\left\{\lambda_0, p^{1/2}g_{\lambda_0}\right\}\right), \quad L(1,1). \tag{27}$$

If $m > 2$, then $L(A)$ is the orthogonal direct sum of the rational subspaces

$$\begin{array}{llll} \mathrm{Ln}(V_m), & \mathrm{Ln}(V_1'), & \mathrm{Ln}(F_A(V_1')), & \mathrm{Ln}\left(\left\{\lambda_0, p^{1/2}g_{\lambda_0}\right\}\right), \\ L(1, m-1), & \mathrm{Ln}(V_j), & \mathrm{Ln}(F_A(V_j)), & 1 < j < m. \end{array}$$

Set

$$R \equiv R(m) \cup \bigcup_{j-1}^{m-1} R^j(m) \cup S^j(m) \cup \left\{\lambda_0, p^{1/2}g_{\lambda_0}\right\} \cup \left\{E_{pk}: 0 \le k < p^{m-2}\right\}. \tag{29}$$

Applying Theorems 1–5 to (27) and (28), we have the next result.

THEOREM 7. *R is a rational basis of $L(A)$.*

A linear transformation Q of $L(A)$ is called rational if Q maps a rational basis of $L(A)$ onto a rational basis. Equivalently, Q is rational if and only if the matrix of Q relative to any rational basis is a rational matrix.

A linear isomorphism P of $L(A)$ is called a permutation if the matrix of P relative to the standard basis of $L(A)$ is a permutation matrix.

The subspace $\mathrm{Ln}(V_m)$ is F_A-invariant. The subspaces $\mathrm{Ln}(V_j)$ and $\mathrm{Ln}(F_A(V_j))$, $1 \le j < m$, are interchanged by the action of F_A. In terms of the rational basis R, a rational linear isomorphism Q of $L(A)$ will be defined such that each of the subspaces given in (27) and (28) are QF_A-invariant.

The action of QF_A "permutes" the elements of V_m, up to a constant multiple given by Gauss sums. The elements of V_j and the elements of $\{g_\lambda: \lambda \in V_j\}$, $1 \le j < m$, are "permuted" by QF_A as well, up to constant multiples given by Gauss sums. A permutation P of $L(A)$ will be defined which mimics QF_A, in a sense made explicit below. This leads to a diagonal matrix representation of PQF_A relative to the basis given in Theorem 7 of Section 5.

Define the linear transformation Q of $L(A)$ by setting Q equal to the identity mapping on the subspace $\mathrm{Ln}(V_m)$ $L(1, m-1)$ and by setting

$$Q(r_k^j) \equiv R_k^j, \quad Q(R_k^j) \equiv r_k^j, \quad 1 \le j < m, 0 \le k < s_j.$$
$$Q(\lambda_0) \equiv p^{1/2}_{\lambda_0}g, \quad Q\left(p^{1/2}_{\lambda_0}g\right) \equiv \lambda_0. \tag{30}$$

Since Q maps the rational basis R onto itself, Q is a rational linear isomorphism of $L(A)$.

LEMMA 1. *If* $m > 1$, $1 \le j < m$, *and* $\lambda \in V_j$, $\lambda \ne \lambda_0$ *then*

$$Q(\lambda) = g_{\lambda^{-1}}, \qquad Q(g_{\lambda^{-1}}) = \lambda. \tag{31}$$

Proof. By Theorems 3 and 4, we have

$$Q(\lambda) = \sum_{k=0}^{s_j-1} \lambda(y^k) Q(r_k^j) = \sum_{k=0}^{s_j-1} \lambda(y^k) R_k^j.$$

The first part of the (31) follows from Theorem 6. The second part of (31) is proved in the same way.

Consider the linear isomorphism QF_A. Note that $QF_A = F_A$ on the subspace $\mathrm{Ln}(V_m) \oplus L(1, m-1)$. If $\lambda \in V_j$, $1 \le j < m$, and $\lambda \ne \lambda_0$, we have by (21) of Section 5,

$$\begin{aligned} QF_A(\lambda) &= p^{m-j} G_j(\psi) \lambda^{-1} \\ QF_A(g_{\lambda^{-1}}) &= p^{j-m} G_j(\psi) g_\lambda, \qquad \lambda = \pi_j^*(\psi). \end{aligned} \tag{32}$$

By (19) of Section 5 we have

$$\begin{aligned} QF_A(\lambda_0) &= -p^{m-1}\lambda_0, \\ QF_A\left(p^{1/2} g_{\lambda_0}\right) &= -p^{1-m}\left(p^{1/2} g_{\lambda_0}\right). \end{aligned} \tag{33}$$

As a consequence of (32) and (33) we have that $\mathrm{Ln}(V_j)$ and $\mathrm{Ln}(F_A(V_j))$, $1 \le j < m$, are QF_A-invariant subspaces. In fact, QF_A permutes V_j and $\{g_{\lambda^{-1}}\colon \lambda V_j\}$.

Let y generate U. Then y^{-1} generates U. Take $0 \le j < m$ and define the mapping α_j of $p^j U$ by the rule

$$\alpha_j(p^j y^k) \equiv p^j y^{-k}, \qquad 0 \le k < t = o(U). \tag{34}$$

The mapping α_j is a bijection of $p^j U$. Extend α_j to a permutation of A by setting α_j equal to the identity mapping on $A - p^j U$. The linear isomorphism P_j of $L(A)$, $0 \le j < m$, given by

$$P_j(f) \equiv f \circ \alpha_j, \qquad 0 \le j < m,\ f \in L(A), \tag{35}$$

is a permutation. Define the permutation P by

$$P = \prod_{j=0}^{m-1} P_j. \tag{36}$$

LEMMA 1.

$$P(\lambda) = \lambda^{-1}, \qquad \lambda \in \hat{U},$$
$$P(g_\lambda) = g_{\lambda^{-1}}, \qquad \lambda \in W_m = \hat{W} - V_m. \tag{37}$$

Proof. Since $\lambda \in \hat{U}$ vanishes from U, we have $p(\lambda) = P_0(\lambda)$, and

$$P_0(\lambda)(y^k) = \lambda(y^{-k}) = \lambda^{-1}(y^k), \qquad 0 \le k < t.$$

Take $\lambda \in W_m$. If $\lambda \in V_j$, $1 \le k < m$, then g_λ vanishes from $p^{m-j}U$ and $P(g_\lambda) = P_{m-j}(g_\lambda)$. Using (10) and (20) of Section 5, the second assertion of the lemma follows.

LEMMA 2. *P restricted to $L(1, m-1)$ is the identity mapping.*

Set

$$F'_A \equiv PQAF_A. \tag{38}$$

The space $\mathrm{Ln}(V_m)$ is F'_A-invariant and if $\lambda \in V_m$ then by Theorem 4 of Section 5 and Lemma 1,

$$F'_A(\lambda) = G_m(\lambda)\lambda. \tag{39}$$

The spaces $\mathrm{Ln}(V_j)$ and $\mathrm{Ln}(F_A(V_j))$, $1 \le j < m$, are F'_A-invariant and by (32), (33) and Lemma 1, we have for $\lambda \in V_j$, $\lambda \ne \lambda_0$,

$$F'_A(g_\lambda) = p^{j-m}G_j(\psi)g \tag{40}$$

and

$$F'_A(\lambda_0) = -p^{m-1}\lambda_0$$
$$F'_A\left(p^{1/2}g_{\lambda_0}\right) = -p^{1-m}\left(p^{1/2}g_{\lambda_0}\right). \tag{41}$$

We also note that $F'_A = F_A$ on $L(1, m-1)$.

Consider again $V' \subset U(1)$, given in (1). Define the diagonal matrix $G(1)$ by the rule

$$G(1) \equiv \left[G_1(\lambda)\right]_{\lambda \in V'}. \tag{42}$$

Define the diagonal matrix $G(m)$ by the rule

$$G(m) \equiv \left[G_m(\lambda)\right]_{\lambda \in V(m)}. \tag{43}$$

We have proved the following results.

THEOREM 8. *The matrix of F'_A restricted to $\mathrm{Ln}(V_m)$ relative to the basis V_m is $G(m)$.*

THEOREM 9. *If $m > 2$ and $1 < j < m$, then the matrix of F_A' restricted to $\mathrm{Ln}(V_j)$ relative to the basis V_j is $p^{m-j}G(j)$ and the matrix of F_A' restricted to $\mathrm{Ln}(F_A(F_j))$ relative to the basis $\{g_{\lambda^{-1}}: \lambda \in V_j\}$ is $p^{j-m}G(j)$.*

THEOREM 10. *The matrix of F_A' restricted to $\mathrm{Ln}(V_1')$ relative to the basis V_1' is $p^{m-1}G(1)$ and the matrix of F_A' restricted to $\mathrm{Ln}(F_A(V_1'))$ relative to the basis $\{g_{\lambda^{-1}}: \lambda \in V_1'\}$ is $p^{1-m}G(1)$.*

Let

$$Y(j) = X(j)G(j)X(j)^{-1}, \qquad 1 \le j < m. \tag{44}$$

Putting together Theorems 8–10 and Theorems 3–5, we have the next result.

THEOREM 11. *The matrix of F_A' relative to the basis R is*

$$Y(m) \oplus Z(m) \oplus \begin{bmatrix} -p^{m-1} & 0 \\ 0 & -p^{1-m} \end{bmatrix} \oplus pF(p^{m-2}), \tag{45}$$

where

$$Z(m) \equiv \sum_{j=1}^{m-1} \left(p^{m-j}Y(j) \oplus p^{j-m}Y(j)\right). \tag{46}$$

The matrices $Y(j)$, $1 \le j \le m$, have a special form which will now be exploited to complete the relation between the matrix description of F_A' given in (45) and the work of Auslander, Feig, and Winograd. The Chinese remainder theorem in a form described in detail in [1] will be used. For completeness, we recall some of the results in [1].

Let $x_0, x_1, \ldots, x_{h-1}$ be distinct complex numbers and form (46) the polynomial

$$g(u) = (u - x_0)(u - x_1) \cdots (u - x_{h-1}).$$

Form the quotient polynomial algebra $\mathbf{C}[u]/g(u)$. As a complex vector space, $\mathbf{C}[u]/g(u)$ has dimension h and the set

$$\{u^k; 0 \le k < r\} \tag{47}$$

is a basis.

A basis $\{\delta_j: 0 \le j < r\}$ of $\mathbf{C}[u]/g(u)$ is called an idempotent basis if

$$\delta_j\delta_k = \begin{cases} i, & j = k, \\ 0, & j \ne k. \end{cases} \tag{48}$$

CHINESE REMAINDER THEOREM. *There exists an idempotent basis of* $\mathbb{C}[u]/g(u)$,

$$\{\delta_j : 0 \le j < h\}, \tag{49}$$

satisfying

$$u^k = \sum_{j=0}^{h-1} x_j^k \delta_j, \qquad 0 \le k < h. \tag{50}$$

Observe that the change of basis matrix taking the basis (49) to the basis (47) is

$$Z \equiv \left[\delta_j^k\right]_{0 \le j,\, k < h}. \tag{51}$$

Also, if $f \in \mathbb{C}[u]/g(u)$, then from (50), we have

$$f = \sum_{j=0}^{h-1} f(x_j)\delta_j. \tag{52}$$

Taking $f \in \mathbb{C}[u]/g(u)$ and let $\gamma(f)$ denote the linear transform of $\mathbb{C}[u]/g(u)$ given by

$$\gamma(f)(h) \equiv fh, \qquad h \in \mathbb{C}[u]/g(u). \tag{53}$$

We call γ the regular representation of $\mathbb{C}[U]/g(u)$. Denote by $R(f)$ the matrix of $\gamma(f)$ relative to the basis (47) and call R the regular matrix representation of $\mathbb{C}[u]/g(u)$.

Take $f \in \mathbb{C}[u]/g(u)$ and let $R'(f)$ denote the matrix of $\gamma(f)$ relative to the idempotent basis (51) of $\mathbb{C}[u]/g(u)$. By (52) and (49), a straightforward computation shows that $R'(f)$ is the diagonal matrix

$$R'(f) = \begin{bmatrix} f(x_0) & & 0 \\ & \ddots & \\ 0 & & f(x_{h-1}) \end{bmatrix}, \qquad f \in \mathbb{C}[u]/g(u). \tag{54}$$

By (51), we have

$$R(f) = Z^{-1}R'(f)Z, \qquad f \in \mathbb{C}[u]/g(u). \tag{55}$$

Consider again the matrix

$$Y(m) = X(m)G(m)X(m)^{-1}, \qquad m \ge 1. \tag{56}$$

Let $v = \exp(2\pi i/t)$, $t = o(U(m))$. Observe that $X(m)$ is the van der

Monde matrix of the set

$$S = \{ v^k : 0 \le k < t,\ p \nmid k \}. \tag{57}$$

The set S has order $s = o(V(m))$.

We have

$$u^t - 1 = \sum_{j=0}^{t-1} (u - v^j). \tag{58}$$

Form the polynomial of degree s:

$$\psi_m(u) = \prod_{r \in S} (u - r), \qquad m \ge 1, \tag{59}$$

and observe that

$$u^t - 1 = \psi_m(u)(u^{t/p} - 1) = \sum_{j=0}^{m} \psi_j(u), \tag{60}$$

where we set $\psi_0(u) \equiv u - 1$.

Consider the field $Q(v)$. The set S is contained in $Q(v)$. Also $Q(v)$ is a Galois extension of Q and S is invariant under the Galois group of the extension $Q(v)/Q$. It follows that

$$\psi_m(u) \in Q[u], \qquad m \ge 1. \tag{61}$$

Form the quotient polynomial algebra $\mathbb{C}[u]/\psi_m(u)$ and denote the regular matrix representation of $\mathbb{C}[u]/\psi_m(u)$ by R_m. Let

$$\{ \delta_j : 0 \le j < t,\ p \nmid j \} \tag{62}$$

be the idempotent basis of $\mathbb{C}[u]/\psi_m(u)$ satisfying

$$u^k = \sum_{0 \le j < t,\ p \mid j} v^{jk} \delta_j, \qquad 0 \le k < s. \tag{63}$$

The change of basis matrix taking the basis (62) to the basis (47) is $X(m)^t$. Then,

$$R_m(f) = \left(X(m)^t \right)^{-1} R'_m(f) X(m)^t, \qquad r \in \mathbb{C}[u]/\psi_m(u), \tag{64}$$

where $R'_m(f)$ is the matrix of the regular representation $\gamma(f)$ relative to the basis (62). We write (64) by taking transposes

$$R_m(f)^t = X(m) R'_m(f) X(m)^{-1}, \qquad f \in \mathbb{C}[u]/\psi_m(u). \tag{65}$$

We have used (54). Define

$$g_m(u) \equiv \sum_{j=0}^{t-1} w^{y^j} u^j, \qquad w = \exp(2\pi i/n),\ n = p^m,\ m \geq 1. \tag{66}$$

Recall, y generates $U = U(m)$. We call $g_m(u)$ the Gauss sum polynomial. Viewing $g_m \in \mathbb{C}[u]/\psi_m(u)$, we have

$$R'_m(g_m) = G(m), \qquad m \geq 1. \tag{67}$$

From (65), (67), and (56), we get the next result.

THEOREM 12. *Let $m \geq 1$ and R denote the regular matrix representation of $\mathbb{C}[u]/\psi_m(u)$, where $\psi_m(u)$ is the rational polynomial defined in* (59). *Then*

$$Y(m) = R_m(g_m)^t, \qquad m \geq 1, \tag{68}$$

where $g_m(u)$ is the Gauss sum polynomial defined in (66).

Theorems 11 and 12 imply

THEOREM 13. *The matrix of F'_A relative to the rational basis R is given by*

$$R_m(g_m)^t \oplus S(m) \oplus \begin{bmatrix} -p^{m-1} & 0 \\ 0 & -p^{1-m} \end{bmatrix} \oplus pF(p^{m-2}), \tag{69}$$

where

$$S(m) \equiv \sum_{j=1}^{m-1} \left(p^{m-j} R_j(g_j)^t \oplus p^{j-m} R_j(g_j)^t \right). \tag{70}$$

If Q_1 is the matrix of PQ relative to the standard basis of $L(A)$ and Q_2 is the change of basis matrix taking R to the standard basis of $L(A)$, then the matrix

$$(Q_2)^{-1} Q_1 F(p^m) Q_2 \tag{71}$$

is given by (69). We can apply Theorem 13 to $F(p^{m-2})$. Continuing in this way, rational non-singular matrices B_1 and B_2 can be found such that the matrix

$$B_1 F(p^m) B_2 \tag{72}$$

is the direct sum of d_j copies of $R_j(g_j)^t$, up to a constant multiple, where

$$d_{m+1-j} = j, \qquad 1 \leq j \leq m, \tag{73}$$

and 2×2 diagonal matrices. This is the main step in [1].

REFERENCES

1. L. AUSLANDER, E. FEIG, AND S. WINOGRAD, The multiplicative complexity of the discrete Fourier transform, *Adv. in Appl. Math.* **5** (1984), 31–55.
2. C. RADAR, Discrete Fourier transforms when the number of data samples is prime, *Proc. IEE-E* **56** (1968), 1107–1108.
3. R. TOLIMIERI, The construction of orthogonal bases diagonalizing the discrete Fourier transform, *Adv. in Appl. Math.* **5** (1984), 56–86.
4. S. WINOGRAD, "Arithmetic Complexity of Computations," CBMS Regional Conf. Ser. in Math. Vol. 33, Soc. Indus. Appl. Math., Philadelphia, 1980.